Republic of the Philippines
NATIONAL POLICE COMMISSION
PHILIPPINE NATIONAL POLICE
ANTI-CYBERCRIME GROUP
Camp BGen Rafael T Crame, Quezon City

ACG-CYBER SECURITY BULLETIN NR 192

ACG-CSB 072820192

Reference Number ACG-CSB 072820192

Beware of Business email compromise attacks

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

SUMMARY

Business email compromise attacks are form of cyber crime which uses email fraud to attack commercial, government and non-profit organizations to achieve a specific outcome which negatively impacts the target organization which includes invoice scams and spear phishing spoof attacks designed to gather data for other criminal activities. Consumer privacy breaches often occur as a result of business email compromise attack.

Typically an attack targets a specific employee roles within an organization by sending a spoof email or series of spoof emails which fraudulently represents a senior colleague (CEO or similar) or a trusted customer. The email will issue instructions, such as approving payments or releasing client data. The email often use social engineering to trick the victim into making money transfers to the bank account of the fraudster.

Business email compromise attacks often use spoofed email addresses, authentic signatures, and logos to look more credible. Even if the message looks like it was sent by someone in your organization or a known vendor, it may not be legitimate. Many Business email compromise attacks phishing emails don’t include links or attachments. These attacks begin with an email that engages the target in conversation known as a knock-knock email. If the target responds, the attacker continues to manipulate the target until they get them to transfer the requested funds or hand over confidential information. Business email compromise attacks also makes last minute change requests to existing wires, with the hopes that you will not verify this request and wire is transmitted per their request.

In Business email compromise attacks schemes emails are not massively sent, they are sent to only a few employees who regularly performs wire transfers, like CFO’s, financial directors, or accountants.

RECOMMENDATION

All PNP personnel as well as the public are advised to follow the tips in order to avoid the risk of Business email compromise attacks, to wit:

- Carefully scrutinize and review all emails especially request for transfer of funds. Be wary of irregular emails that are sent from C-suite executives, as they are used to trick employees into acting with urgency.
- Educate and train employees, they are the biggest asset of the company and also they are the weakest link when it comes to security. Invest and commit in training employees according to the best practices of the company.
- Verify any changes in vendor payment location by using a secondary sign-off by company personnel
- Stay updated on your customers' habits including the details, and reasons behind payments.
- Confirm requests for transfer of funds when using phone verification as part of two-factor authentication, use known familiar numbers and not the details provided in the email requests.

For additional information, please refer to the following websites:

- https://en.wikipedia.org/wiki/Business_email_compromise
- https://www.opusbank.com/business-email-compromise-schemes
- https://www.opusbank.com/business-email-compromise-schemes
- https://www.lexology.com/library/detail.aspx?g=9b3f995b-cf86-47cc-bd71-dfd40ae7fe16
- https://www.barracuda.com/glossary/business-email-compromise
- https://www.ftc.gov/tips-advice/business-center/guidance/scams-your-small-business-guide-business
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes

POINT OF CONTACT

Please contact PMAJ JOSEPH ARVIL L VILLARAN, Police Communication Relation officer thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.